Access controls worksheet

	Note(s)	Issue(s)	Recommendation(s)
Authorization /authentication	**Objective:** List 1-2 pieces of information that can help identify the threat: ● *Who caused this incident?* ○ *Robert Taylor Jr.* ● *When did it occur?* ○ *8:29:57 am (5 days ago)* ● *What device was used?* ○ *Computer: Up2-NoGud* ○ *152.207.255.255*	**Objective:** Based on your notes, list 1-2 authorization issues: ● *What level of access did the user have?* ○ *Administrator* ● *Should their account be active?* ○ *No, because they ended employment on 12/27/2019.* ○ *The incident log shows they accessed the system in 2023.*	**Objective:** Make at least 1 recommendation that could prevent this kind of incident: ● *Which technical, operational, or managerial controls could help?* ○ *Technical control: Implement Role-Based Access Control (RBAC) to ensure only authorized HR personnel can make payroll changes.* ○ *Operational control: Disable shared or default administrator accounts for regular use; require named user accounts with specific roles* ○ *Managerial control: Enforce a least privilege policy and perform regular user access reviews to remove unnecessary permissions and deactivate inactive accounts.* ○ *Set up an automation rule to **immediately revoke user permissions** after their **employment end date**.*